Nimi: _____ Päivämäärä: _____ Pisteet: _____

Mikä on VPN Tehtävämoniste

Käytännön harjoituksia verkkoprotokollista, tunneloinnista ja tietoturvakontrolleista.

VPN, OPPIMISEN YLEISKATSAUS

OPPIJA
OPISKELIJASTATUS
Verkon puolustajan polku

TURVALLINEN
YHTEYDEN TILA
Datapakettien suojaaminen

AKTIIVINEN
VUOTOSUOJA
DNS- ja IPv6-vuodonesto

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: virtuaalisten yksityisverkkojen (VPN) perusperiaatteet. Tutustut siihen, miten salatut tunnelit suojaavat tietojasi, miten verkkoprotokollat toimivat ja miten tunnistat ja ehkäiset yksityisyysvuotoja.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse VPN-käsitteet ja -protokollat.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin VPN-opas

URL: https://www.vpn.com/fi/vpn/

Oppimispolkusi: VPN

- Selitä datan tunneloinnin ja kapseloinnin käsite.
- Tunnista tavalliset protokollamääritykset ja salausmenetelmät.
- Analysoi palvelimien ja IP-osoitteen peittämisen roolia virtuaalisissa yksityisverkoissa.
- Ymmärrä, miten palveluntarjoajat seuraavat selailua ja miten VPN estää sen.
- Erota toisistaan virtuaaliverkkotopologian toiminnalliset rajat.

MIKÄ ON VPN -OPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: tosielämän tilanteet tapaustutkimusosiossa. Lopuksi bonustehtävä Nopeat vastaukset.

MIKÄ ON VPN? (JOHDANTO)

Virtuaalinen yksityisverkko on enemmän kuin pelkkä yksityisyyskytkin. Se on salattu tunneli, joka reitittää internetliikenteesi etäpalvelimen kautta. Tämä piilottaa IP-osoitteesi, estää internetoperaattoriasi kokoamasta lokeja verkkotoimistasi ja suojaa tietosi julkisissa verkoissa. Terminologian ymmärtäminen on olennaista digitaalisen turvallisuuden ylläpitämiseksi.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mikä on virtuaalisen erillisverkon (VPN) ensisijainen tehtävä?**

- A. Nopeuttaa internetselaimen renderöintiä
- B. Salata datapaketit ja peittää julkinen IP-osoitteesi
- C. Verkkosivuston evästetietokantojen tallentaminen paikallisesti
- D. Fyysisen tietokonelaitteistosi korvaamiseksi

2 **2. Mitä on verkkotunnelointi VPN:n yhteydessä?**

- A. Päällekkäisten verkkolokitiedostojen poistaminen
- B. Paikallisten tietokantojen tallennustiedostojen asentaminen
- C. Tiedostojen jakaminen muiden paikallisten tietokoneiden kanssa
- D. Yhden verkkopaketin kapselointi toisen suojatun paketin sisään

3 **3. Mitä salausstandardia käytetään laajalti VPN-liikenteen suojaamiseen?**

- A. Vanhentunut DES-salaus
- B. Moderni AES-256-standardi
- C. Selväkielinen base64-koodaus
- D. Tavallinen rot13-salakirjoitus

4 **4. Mikä verkkoliikenteesi osa on VPN:n salaama?**

- A. Vain paikallisen laiteverkon tulostustyöt
- B. Fyysisen Ethernet-kaapelin reitityspolku
- C. Verkkopaketin koko hyötykuorman osa
- D. Vain selaimesi hakuhistoriat

5 **5. Mitä termi 'salaus' tarkoittaa verkoissa?**

- A. Selkokielisen datan muuntaminen lukukelvottomaksi salatuksi tekstiksi
- B. Vanhojen viestintätietueiden poistaminen
- C. Paikallisten kaistanleveysrajoitusten nostaminen
- D. Tietokannan käyttöavainten jakaminen julkisesti

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. VPN salaa liikenteesi, mikä estää paikallisen salakuuntelun julkisessa Wi-Fi-verkossa.

○ Tosi ○ Epätosi

7 Kysymys 7

7. VPN muuttaa fyysisesti reitittimesi laitteistoasetuksia.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Tunnelointiprotokollat käärivät datapaketit salattuun siirtokerrokseen.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Symmetrinen salaus käyttää samaa avainta liikenteen salaamiseen ja purkamiseen.

○ Tosi ○ Epätosi

10 Kysymys 10

10. VPN:n käyttö tekee internetyhteydestäsi fyysisesti immuunin kaikille offline-sähkökatkoille.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Liikenteesi suojaamiseksi VPN käärii datapakettisi toisen protokollan sisään; prosessin nimi on _____ .

2. Jos suoratoiston aikana lataus on hidasta, syynä voi olla rajallinen verkon _____ .

3. Vain tietyssä maassa saatavilla oleva suoratoistopalvelu rajoittaa maailmanlaajuisia käyttäjiä esteellä, jonka nimi on _____ .

4. Salaus- ja yhteysparametrit määrittelevät yhteyssäännöt ovat VPN:n _____ .

5. Tietokoneesi paikallinen verkkoliikennettä valvova ja vaaralliset yhteydet estävä suojajärjestelmä on _____ .

6. Kun muodostat VPN-yhteyden, datasi reititetään etätietokoneen kautta julkisen IP-osoitteesi piilottamiseksi; tämä etätietokone on _____ .

SANASTON SANAPANKKI

ALUEESTO KAISTANLEVEYS OPERAATTORI PALOMUURI PALVELIN
PROTOKOLLA TUNNELOINTI YKSITYISYYS

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Verkkokäsitteiden yhdistäminen

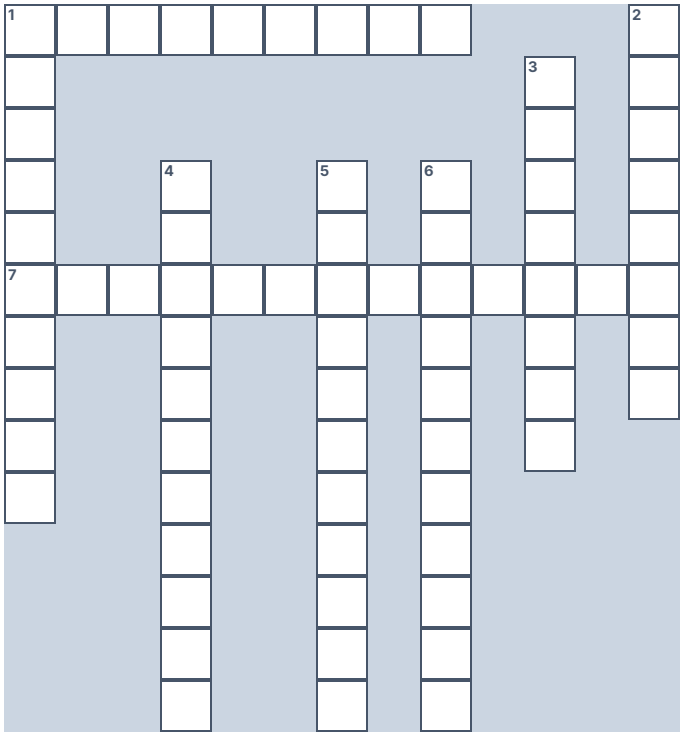
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. Tunnelointi	A	Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi.
☐	2. Protokolla	B	Internetpalveluntarjoaja, joka kuljettaa liikennettäsi ja voi nähdä salaamattoman toiminnan.
☐	3. Kaista	C	Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella.
☐	4. Palvelin	D	Suojausjärjestelmä, joka valvoo ja estää luvattoman liikenteen.
☐	5. Maantieteellinen esto	E	Sääntöjoukko, joka määrittää, miten tietoja siirretään verkossa.
☐	6. Palomuuri	F	Tila, jossa ei ole seurannan tai julkisen valvonnan kohteena.
☐	7. Yksityisyys	G	Tiedonsiirron suurin nopeus yhteyden yli.
☐	8. Internetoperaattori	H	Datapakettien kääriminen toisen paketin sisään turvallista siirtoa varten.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

1. Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9)

7. Yhteyden suurin tiedonsiirtonopeus (13)

PYSTYSUORAAN

1. Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10)

2. Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8)

3. Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8)

4. Tila, jossa ei ole seurantaa eikä julkista valvontaa (11)

5. Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11)

6. Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

1 vaakasuoraan: Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9 kirjainta):

7 vaakasuoraan: Yhteyden suurin tiedonsiirtonopeus (13 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10 kirjainta):

2 pystysuoraan: Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8 kirjainta):

3 pystysuoraan: Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8 kirjainta):

4 pystysuoraan: Tila, jossa ei ole seurantaa eikä julkista valvontaa (11 kirjainta):

5 pystysuoraan: Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11 kirjainta):

6 pystysuoraan: Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

Y	K	S	I	T	Y	I	S	Y	Y	S	T	Ä	B	I
I	N	Ö	I	R	U	U	M	O	L	A	P	H	K	A
T	P	R	P	Z	C	N	Ö	Ä	G	Å	Q	Y	L	X
N	M	X	R	B	P	Y	V	N	H	X	D	U	Ä	X
I	R	O	T	T	A	A	R	E	P	O	E	L	T	B
O	Z	Ö	Å	N	T	S	Å	J	Q	E	E	A	D	L
L	S	Y	Z	Z	M	K	I	W	S	I	G	B	F	J
E	L	V	U	Y	T	Ö	F	T	I	F	U	C	A	M
N	R	C	Ö	N	L	Y	O	T	W	A	U	Z	K	N
N	N	H	I	N	I	L	E	V	L	A	P	O	I	T
U	K	A	I	S	T	A	N	L	E	V	E	Y	S	G
T	M	V	M	T	Z	I	B	W	G	Ä	P	Ä	Z	U
I	V	P	R	O	T	O	K	O	L	L	A	Å	A	R
X	P	P	Ö	Q	J	R	V	I	R	X	W	Q	W	W
L	A	F	Q	O	M	B	P	X	G	H	R	S	Z	Ä

SANASTOLISTA

TUNNELOINTI PROTOKOLLA KAISTANLEVEYS PALVELIN ALUEESTO
PALOMUURI YKSITYISYYS OPERAATTORI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. TUNNELOINTI**
- **B. PROTOKOLLA**
- **C. KAISTANLEVEYS**
- **D. PALVELIN**
- **E. ALUEESTO**
- **F. PALOMUURI**
- **G. YKSITYISYYS**
- **H. OPERAATTORI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa.
2. Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella.
3. Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen.
4. Tila, jossa ei ole seurantaa eikä julkista valvontaa.
5. Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu.
6. Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten.
7. Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi.
8. Yhteyden suurin tiedonsiirtonopeus.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä VPN-käsitteitä ja -termejä. Kirjoita vastauksesi täytettäviin syöttökenttiin.

1. EOTULITNNIN
2. YTAAIKENSE VLS
3. ELAESOTU
4. IYSYSTYSYKI
5. LKARTOOPLO
6. INVLPEAL
7. UPRIUOAML
8. OTIAEOAPRT R

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Asioita, jotka IP-osoite voi paljastaa			
2	Myyttejä VPN:istä			
3	Asioita, jotka kulkevat internetin halki			
4	Lupauksia, joita hyvä VPN-palveluntarjoaja antaa			
5	Salaisuuksia, jotka salaisit			
6	Asioita, joilta VPN ei voi suojata sinua			
7	Tapoja tunnistaa väärennetty Wi-Fi-verkko			
8	Yksityisyyteen liittyviä sanoja			
9	Laitteita, jotka voivat käyttää VPN:ää			
10	Asioita, jotka tapahtuvat, kun painat "Yhdistä"			
11	Paikkoja, joissa käyttäisit VPN:ää			
12	Syitä käyttää VPN:ää matkustaessa			
13	Tosielämän asioita, jotka näyttävät tunnelilta			
14	Sanoja tästä tehtävämonisteesta, jotka haluat muistaa			
15	Sanoja, joilla selittäisit VPN:n lapselle			

Tarkistuspiste 8: VPN:n tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

SARAH (KAHVILAN OPISKELIJA)

👷 "Hei! Istun Coffee & Bytesissa. Täällä on suojaamaton julkinen verkko nimeltä 'Free_Wi-Fi_No_Password'. Haluan kirjautua koulun sähköpostiin ja lähettää tehtäväni, mutta pelkään hakkereita. Mitä riskejä tämän verkon käyttöön liittyy ilman VPN:ää, ja miten VPN suojaa tietoni?"

ALEX (MATKAILIJAOPISKELIJA)

👷 "Voi ei! Matkustan ulkomailla projektin vuoksi ja yritän katsoa biologiadokumenttia, joka on isännöity kotimaassani olevalla palvelimella. Sivusto kuitenkin sanoo 'Tämä video ei ole saatavilla nykyisessä sijainnissasi.' Miksi minut on estetty, ja miten VPN voi auttaa katsomaan sen?"

Tarkistuspiste 9: Salakirjoituksen purkaminen

VPN salaa liikenteesi sen suojaamiseksi. Käytä alla olevaa kirjain–numero-avainta purkaaksesi kyberturvallisuusviestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

19 21 15 10 1 1

25 11 19 9 20 25 9 19 25 25 20 5 19 9

20 21 18 22 1 12 12 9 19 5 12 12 1

20 21 14 14 5 12 9 12 12 1

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa A)

Tutustu yleisimpiin kysymyksiin ja vastauksiin, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q1: Mikä on VPN ja miten se toimii?

Virtuaalinen yksityisverkko (VPN) salaa internetyhteytesi ja reitittää liikenteesi suojatun etäpalvelimen kautta. Tämä peittää julkisen IP-osoitteesi ja rajoittaa sitä, mitä paikallisverkon tarkkailijat ja internetoperaattorisi näkevät VPN-tunnelin kautta kulkevasta liikenteestä.

Q2: Miksi minun pitäisi käyttää VPN:ää?

VPN suojaa digitaalista yksityisyyttäsi, turvaa yhteytesi julkisissa Wi-Fi-verkoissa (kuten kahviloissa tai lentokentillä), voi vähentää toimintaan perustuvaa kuristusta, kun operaattori ei pysty tunnistamaan salatun liikenteen tyyppiä, ohittaa maantieteelliset rajoitukset globaalin sisällön käyttämiseksi ja auttaa suojaamaan etätyön resursseja.

Q3: Tekeekö VPN minusta täysin nimettömän verkossa?

Ei. Vaikka VPN piilottaa IP-osoitteesi ja salaa liikenteen, sinua voidaan silti seurata selainevästeillä, aktiivisilla tileillä (kuten Google tai Facebook), selaimen sormenjäljillä tai jos VPN-palveluntarjoajasi kirjaa tietosi.

Q4: Hidastaako VPN internet-yhteyteni nopeutta?

Kyllä, hieman. Salausprosessi ja fyysinen etäisyys VPN-palvelimeen lisäävät viivettä ja kuormaa. Vaikutus vaihtelee palveluntarjoajan, protokollan, palvelimen etäisyyden, laitteen ja verkko-olosuhteiden mukaan.

Q5: Onko VPN:n käyttö laillista?

VPN:n käyttö on laillista monissa maissa, mutta jotkin lainkäyttöalueet rajoittavat, sääntelevät tai estävät VPN-palveluja. Käyttäjien tulisi tarkistaa voimassa olevat paikalliset lait ennen käyttöä. Lisätietoja saat VPN.comin laillisuusoppaista.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, perustaso (Osa B)

Tutustu yleisimpiin kysymyksiin ja vastauksiin, joita mahdolliset asiakkaat esittävät virtuaalisten yksityisverkkojen käytöstä.

Q6: Voinko käyttää ilmaista VPN:ää?

Ilmaiset VPN:t voivat perustua mainontaan, rajoitettuihin ominaisuuksiin, käyttöanalytiikkaan, datakattoihin tai muihin tulonhankintamalleihin. Käyttäjien tulisi tarkistaa palveluntarjoajan tietosuojakäytäntö, omistus, auditoinnit ja liiketoimintamalli ennen käyttöä.

Q7: Mikä on "ei lokeja" -käytäntö?

Lokittomuuskäytäntö kuvaa, mitä toiminta- ja yhteystietoja palveluntarjoaja ilmoittaa olevansa säilyttämättä. Tarkka laajuus vaihtelee, joten lukijoiden tulisi tarkistaa käytäntö ja riippumattomien auditointien havainnot.

Q8: Miten valitsen parhaan VPN:n?

Etsi auditoituja lokittomuuskäytäntöjä, vahvoja protokollia (WireGuard, OpenVPN), turvallisia palvelinsijainteja, nopeita yhteyksiä, vain RAM-muistia käyttäviä palvelimia, kill switch -toiminto ja lainkäyttöalue tiedusteluyhteistyöliittoumien (kuten 5/9/14 Eyes) ulkopuolella.

Q9: Voinko käyttää VPN:ää puhelimessani ja älytelevisiossani?

Kyllä. Nykyaikaiset VPN-palveluntarjoajat tarjoavat omat sovellukset iOS:lle, Androidille, macOS:lle, Windowsille, Linuxille ja älytelevisioille sekä reititinasennuksia, jotka suojaavat kaikkia kotiverkkosi laitteita.

Q10: Mikä on kill switch?

Kill Switch on tietoturvaominaisuus, joka katkaisee laitteesi internetyhteyden automaattisesti, jos VPN-yhteys katkeaa. Tämä estää salaamattomien tietojesi tai todellisen IP-osoitteesi vuotamisen.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa C)

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q1: Mikä ero on WireGuardilla, OpenVPN:llä ja IKEv2:lla?

WireGuard on nykyaikainen, kevyt protokolla (vain noin 4 000 koodiriviä), joka tarjoaa nopeat nopeudet ja lyhyet yhteysajat. OpenVPN on erittäin turvallinen, käytännössä koeteltu avoimen lähdekoodin protokolla. IKEv2 sopii erinomaisesti mobiililaitteille, koska se osaa yhdistää nopeasti uudelleen verkkoa vaihdettaessa. [4]

Q2: Mitä on kaksois-VPN tai Multi-Hop-reititys?

Multi-Hop reitittää liikenteesi kahden tai useamman VPN-palvelimen kautta peräkkäin. Tämä lisää toisen salauskerroksen ja auttaa pitämään todellisen IP-osoitteesi piilossa toiselta hypyltä, jos yksi palvelin vaarantuu.

Q3: Mitä WebRTC-vuoto on ja miten VPN estää sen?

WebRTC on selainprotokolla, joka voi paljastaa oikeat paikalliset ja julkiset IP-osoitteesi, vaikka VPN olisi käytössä. Premium-VPN:t estävät tai väärentävät WebRTC-pyyntöjä pöytäkone- ja mobiilisovelluksissaan sekä selainlaajennuksissaan.

Q4: Mitä pelkkää RAM-muistia käyttävät palvelimet ovat ja miksi niillä on merkitystä?

Perinteiset palvelimet kirjoittavat dataa kiintolevyille, jotka voidaan takavarikoida tai vaarantaa. Pelkkää RAM-muistia käyttävät (levyttömät) palvelimet toimivat kokonaan haihtuvassa muistissa (RAM). Kun palvelin käynnistetään uudelleen tai sammutetaan, muistissa oleva data pyyhkiytyy.

Q5: Miten obfuskointi ohittaa VPN-estot?

Hämäys (eli "Stealth VPN") naamioi VPN-liikenteen tavalliseksi HTTPS-liikenteeksi (portti 443). Tämä voi auttaa pääsemään ohi syväpakettitarkastuksen (DPI), jota hallitukset tai koulu- ja toimistoverkot käyttävät VPN-yhteyksien estämiseen.

Tarkistuspiste 10: Usein kysytyt kysymykset VPN:stä, jatkotaso (Osa D)

Tutustu virtuaalisten yksityisverkkojen ja suojattujen tunnelointiprotokollien teknisiin ja rakenteellisiin puoliin.

Q6: Mitä jaettu tunnelointi on ja milloin sitä kannattaa käyttää?

Jaetun tunneloinnin avulla voit valita, mitkä sovellukset reitittyvät salatun VPN-tunnelin kautta ja mitkä yhdistävät suoraan internetiin. Käytä sitä reitittääksesi arkaluonteiset pankkisovellukset VPN:n kautta, kun paikalliset pelit yhdistävät suoraan, jolloin vältät VPN:n aiheuttaman viiveen.

Q7: Miten eteenpäin salassapito (Perfect Forward Secrecy) toimii?

PFS varmistaa, että jokaiselle istunnolle luodaan yksilöllinen, väliaikainen salausavain. Vaikka yksityinen avain vaarantuisi tulevaisuudessa, sitä ei voi käyttää menneiden tai tulevien istuntojen purkamiseen, koska ne käyttivät toisistaan riippumattomia avaimia.

Q8: Mitä 5/9/14 Eyes -liittoumat ovat ja miksi minun pitäisi välittää niistä?

Lainkäyttövalta voi vaikuttaa oikeudelliseen menettelyyn, jonka palveluntarjoaja voi kohdata, mutta käytännön yksityisyysriski riippuu myös siitä, mitä tietoja palveluntarjoaja säilyttää, sen teknisestä arkkitehtuurista, omistuksesta, läpinäkyvyysraportoinnista ja auditointihistoriasta.

Q9: Mitä DNS-vuotosuoja on?

DNS-vuodonesto pakottaa laitteesi lähettämään verkkosivujen hakukyselyt (DNS-kyselyt) VPN:n yksityisten, salattujen DNS-palvelimien kautta internetpalveluntarjoajasi palvelimien sijaan. Tämä estää internetpalveluntarjoajaasi seuraamasta, mitä sivustoja vierailet.

Q10: Voiko VPN ohittaa internetpalveluntarjoajan nopeuden rajoituksen?

Joskus. VPN voi auttaa, kun internetpalveluntarjoaja hidastaa valikoiden tunnistettavia toimintoja, mutta se ei ratkaise verkon ruuhkaa, datarajoituksia, tilikohtaisia nopeusrajoituksia tai heikkoa verkon laatua.

Osa 11: 10 mielenkiintoista VPN-faktaa ja tosielämän havaintoa

Tutustu näihin erittäin hyödyllisiin, todellisiin tosiasioihin ja oivalluksiin VPN:ien historiasta, markkinoista ja teknologiasta.

1. ENSIMMÄINEN VPN-PROTOKOLLA

PPTP:n (Point-to-Point Tunneling Protocol) kehitti toimittajaryhmä, johon kuuluivat muun muassa Microsoft, ja se julkaistiin RFC 2637:nä heinäkuussa 1999 etäkäyttö-VPN-yhteyksien tukemiseksi. [6]

2. MARKKINA-ARVO

Maailmanlaajuiset VPN-markkinat ovat kasvaneet nopeasti etätyövaatimusten ja yritysten tietoturvatarpeiden lisääntymisen ansiosta.

3. WIREGUARD-VALLANKUMOUS

WireGuardin koodipohja on erittäin virtaviivainen ja suunniteltu tehokkuutta silmällä pitäen, minkä vuoksi sen tietoturvahaavoittuvuudet on helpompi auditoida kuin perinteisten protokollien. [4]

4. TIUKAT TARKASTUSSTANDARDIT

Johtavat VPN-palveluntarjoajat palkkaavat ulkopuolisia auditoijia (kuten Cure53 tai PwC) tekemään riippumattomia koodikatselmuksia ja varmistamaan, etteivät ne kirjaa käyttäjien toimintaa.

5. 5-EYES-LIITTOUMAN ALKUPERÄ

Five Eyes -liittouma kasvoi vuoden 1946 UKUSA-signaalitiedustelusopimuksesta Yhdysvaltojen ja Britannian välillä, ja siihen liittyivät myöhemmin Kanada, Australia ja Uusi-Seelanti.

6. SYVÄ PAKETTITARKASTUS

Syväpakettitarkastus (DPI) tutkii pakettien sisältöä ja liikennemalleja, ei vain otsikoita, ja jotkin palomuurit käyttävät sitä tavallisten VPN-protokollien tunnistamiseen ja estämiseen.

7. YRITYSKÄYTTÖ

Suuri osa yritysten työntekijöistä maailmanlaajuisesti käyttää suojattuja VPN-yhteyksiä kirjautuakseen sisäisiin tietokantoihin, mikä tekee siitä keskeisen tietoturvastandardin.

8. HAJAUTETUT VPN:T

Hajautetut VPN:t (dVPN) jakavat liikenteen vertaisten ylläpitämien solmujen verkkoon, mikä vähentää riippuvuutta yhdestä keskitetystä palveluntarjoajasta.

9. TOR VS. VPN-ANONYMITEETTI

VPN tunneloi liikenteen yhden palveluntarjoajan kautta, kun taas Tor (The Onion Router) lähettää liikenteen kolmen vapaaehtoisen välityssolmun (sisääntulo, keski ja poistuminen) kautta, jolloin yksikään solmu ei tiedä molempia päitä.

10. TIETOVUOTOJEN KUSTANNUKSET

Nollaluottamusmallin mukaisen suojatun käyttöoikeusmallin käyttö VPN:n kanssa auttaa organisaatioita suojaamaan immateriaalioikeuksia ja lieventämään tietomurtojen taloudellisia vaikutuksia.

Tekniset viitteet ja lähteet

Tässä tehtävämonisteessa käytetyt lainatut julkaisut, salausmääritykset ja viralliset asiakirjastandardit.

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Vastausavain: Mikä on VPN -tehtävämoniste

1 **Päätoiminto** PROTOKOLLAT **Oikea vastaus: B**

OPETTAJALLE

VPN:n päätehtävä on luoda salattu tunneli, joka suojaa pakettien hyötykuormatietoja ja peittää käyttäjän julkisen IP-osoitteen. Lähde: IETF Tunnel RFC.

2 **Verkkotunnelointi** VIIVE **Oikea vastaus: D**

OPETTAJALLE

Tunnelointiprotokollat kapseloivat alkuperäiset datapaketit ulompien kuljetuspakettien sisään, jotta ne voivat kulkea turvallisesti julkisten verkkojen läpi. Lähde: IETF Tunnel RFC.

3 **Kysymys 3** **Oikea vastaus: B**

OPETTAJALLE

Mitä salausstandardia käytetään laajalti VPN-liikenteen suojaamiseen? → Moderni AES-256-standardi

4 **Salatut komponentit** REITITYKSEN HALLINTA **Oikea vastaus: C**

OPETTAJALLE

VPN salaa IP-datapakettien koko hyötykuormaosan ja pitää siirron sisällön luottamuksellisena. Lähde: IETF Tunnel RFC.

5 **Kysymys 5** **Oikea vastaus: A**

OPETTAJALLE

Salaus käyttää algoritmia ja avainta muuttaakseen selkotekstin lukukelvottomaksi salatekstiksi.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Salakuuntelun esto** IP-PEITTO — **Oikea vastaus: Tosi**

OPETTAJALLE

Salatut tunnelit varmistavat, että pakettien hyötykuormat pysyvät lukukelvottomina paikallisia Wi-Fi-verkkoja salakuunteleville toimijoille. Lähde: Deloitte Advisory.

7 **Laitteistomuutokset** NOPEUDET — **Oikea vastaus: Epätosi**

OPETTAJALLE

VPN:t ovat ohjelmistopohjaisia verkkotunneleita, eivätkä ne muuta fyysisesti yhdyskäytäväreitittimesi laitteistoa. Lähde: Cure53 Audit.

8 **Pakettien tunnelointi** NUUSKINTARISKI — **Oikea vastaus: Tosi**

OPETTAJALLE

Tunnelointi toimii käärimällä alkuperäiset verkkopaketit siirto-otsikoiden sisään kuljetusta varten. Lähde: IETF Tunnel RFC.

9 **Symmetriset avaimet** PALOMUURIT — **Oikea vastaus: Tosi**

OPETTAJALLE

Symmetrinen kryptografia käyttää jaettua avainta sekä verkkovirtojen salaamiseen että purkamiseen. Lähde: WireGuard Project.

10 **Virtaimmuniteetti** LOKITON — **Oikea vastaus: Epätosi**

OPETTAJALLE

VPN salaa vain aktiiviset yhteyssignaalit; se ei voi estää paikallisten sähkökatkosten aiheuttamia palvelukatkoja. Lähde: EDRi Retention Guidelines.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

H 1. Tunnelointi	E 2. Protokolla	G 3. Kaista	A 4. Palvelin
C 5. Maantieteellinen esto	D 6. Palomuuri	F 7. Yksityisyys	B 8. Internetoperaattori

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TUNNELOINTI	2 KAISTANLEVEYS	3 ALUEESTO	4 PROTOKOLLA
5 PALOMUURI	6 PALVELIN		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 B – PROTOKOLLA	2 E – ALUEESTO	3 F – PALOMUURI	4 G – YKSITYISYYS
5 H – OPERAATTORI	6 A – TUNNELOINTI	7 D – PALVELIN	8 C – KAISTANLEVEYS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

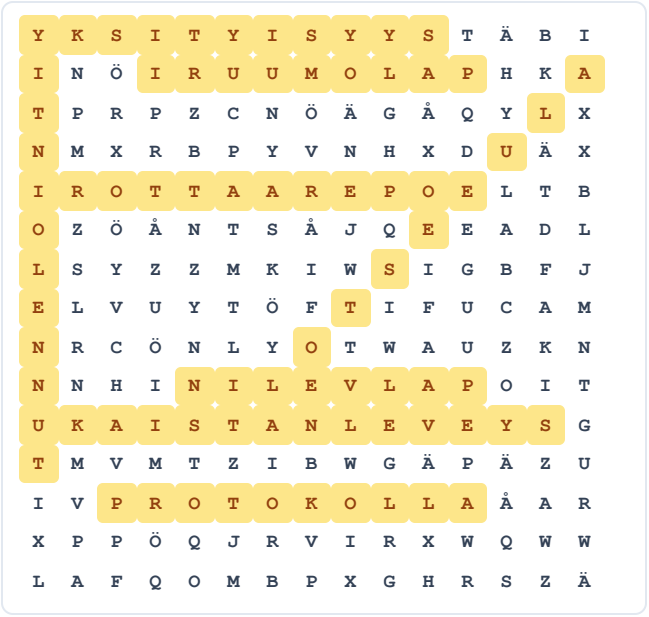
Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Tunnelointi, Protokolla ja Kaista omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

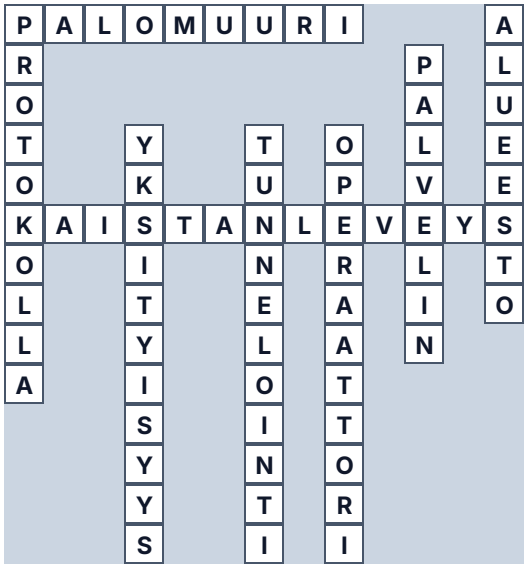
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU



RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

1 vaakasuoraan: PALOMUURI Tietoturvajärjestelmä, joka valvoo ja estää luvattoman liikenteen (9 kirjainta)

7 vaakasuoraan: KAISTANLEVEYS Yhteyden suurin tiedonsiirtonopeus (13 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: PROTOKOLLA Sääntöjoukko, joka määrittää, miten dataa siirretään verkossa (10 kirjainta)

2 pystysuoraan: ALUEESTO Rajoitus, joka estää verkon käytön fyysisen sijainnin perusteella (8 kirjainta)

3 pystysuoraan: PALVELIN Etätietokone, joka reitittää liikenteesi ja peittää IP-osoitteesi (8 kirjainta)

4 pystysuoraan: YKSITYISYYS Tila, jossa ei ole seurantaa eikä julkista valvontaa (11 kirjainta)

5 pystysuoraan: TUNNELOINTI Datapakettien käärimistä toisen paketin sisään turvallista siirtoa varten (11 kirjainta)

6 pystysuoraan: OPERAATTORI Internet-palveluntarjoaja, joka kirjaa liikenteesi lokiin, ellei sitä ole salattu (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. E O T U L I T N N I N — **TUNNELOINTI**
2. Y T A A I K E N S E V L S — **KAISTANLEVEYS**
3. E L A E S O T U — **ALUEESTO**
4. I Y S Y S T Y S Y K I — **YKSITYISYYS**
5. L K A R T O O P L O — **PROTOKOLLA**
6. I N V L P E A L — **PALVELIN**
7. U P R I U O A M L — **PALOMUURI**
8. O T I A E O A P R T R — **OPERAATTORI**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA YKSITYISYYTESI TURVALLISELLA TUNNELILLA"

Tapaustutkimusten vastausavain

A Tilanne A: Julkisen verkon turvallisuus

NUUSKINTA JA SALAUS | Sarahin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Riskit: Pakettien nuuskinta, tietojen sieppaus ja man-in-the-middle-hyökkäykset. Joku samassa kahvilaverkossa voisi kaapata hänen kirjautumistietonsa tai kotitehtävätiedostonsa.
- VPN-suojaus: Salaa verkkopakettien hyötykuormat, jolloin siepattu tunneliliikenne on lukukelvotonta passiivisille paikallisverkon urkkijoille, kun VPN on määritetty oikein.

B Tilanne B: Estettyjen resurssien käyttäminen

MAANTIETEELLISET ESTOT JA IP-OSOITTEET | Alexin dilemma

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Miksi estetty: Suoratoistopalvelu käyttää maantieteellistä estoa, joka yhdistää matkustajan paikallisen IP-osoitteen hänen fyysiseen maahansa ja estää sen aluekohtaisten lisenssien perusteella.
- Miten VPN auttaa: Hän peittää todellisen sijaintinsa reitittämällä liikenteen kotimaansa palvelimen kautta. Sivusto näkee kotimaan IP-osoitteen, mikä sallii pääsyn.